Healthpoint

Information from the Division of Health Care Finance and Policy

Argeo Paul Cellucci
Governor

William D. O'Leary
Secretary, Executive Office
of Health & Human Services

Division of Health Care
Finance and Policy

Two Boylston Street
Boston, MA 02116
(617) 988-3100

Barbara Erban Weinstein
Commissioner

Vol. 3 No. 1 September 1997

HEALTH CARE IN THE INFORMATION AGE: PROTECTING PRIVACY AND INFORMATION

Information or privacy? The debate over collection and use of personally identifiable health data has focused on a trade-off between the two. "Health data" means records of an individual's medical care as well as general information such as gender, age, area of residence, and insurer. Clinical information may include a medical history, details about lifestyle (smoking, alcohol intake, risk behaviors), and treatment history. Though paper records are not immune from mishandling, the increased computerization of this personal information has raised public anxiety. Privacy advocates and patients are concerned that sensitive information, such as identifiable medical records, may now be accessed instantly and shared widely over computer networks. This issue of *Healthpoint* looks at the many uses of health data, considers the privacy concerns over database technology and access to information, and highlights existing and proposed policies that are designed to preserve both data and privacy, rather than one over the other.

Health Data Uses & Benefits

The information collected from an individual's visits to a primary care provider, specialist or hospital is used most often in treatment decisions. Increasingly, it is also used by other health care-related entities for non-clinical purposes. Insurers may use the information, with identifiers, to determine payment for clinical services. When multiple cases are aggregated, health data offer researchers insight into health concerns of specific populations — not individual patients — and provide information for quality of care and cost containment initiatives. The resulting products — epidemiological studies, information on the use of health care services, and the like — are often used by public officials to shape public policy or by health care providers to improve delivery of services.

Health data have been collected and used for public health purposes for hundreds of years. As early as 1741, tavern keepers in Rhode Island were instructed to report patrons with contagious diseases to local authorities. National mortality statistics were first published in 1850. The eradication of smallpox in the early twentieth century was made possible through collection of information on persons with the disease and vaccination of those who may have been exposed. More recent efforts, such as public health campaigns around smoking cessation and cancer screening, all rely on health data to target their messages. This type of close and continuous observation and investigation

into a population's health helps policy makers allocate resources and focus interventions in areas with the greatest need.

Aggregate health data are also used by public policy analysts to evaluate, for example, services for underserved populations, or by employers to compare managed care plans with which they contract. Public agencies, like the state Division of Health Care Finance and Policy and Department of Public Health, and the federal Health Care Financing Administration and Agency for Health Care Policy and Research, publish reports that health care systems put to use in promoting the efficient use of resources and improving the quality of clinical care. These and other agencies are also sources of data for health services researchers, whose disinterested, academically rigorous work benefits health systems and the public's health.

Privacy Concerns

When in the wrong hands or used by the wrong persons, this "benevolent" information can have harmful repercussions. In Tampa, Florida for example, a public health employee released a list of identifiable HIV patients to a newspaper reporter. If health data identifies patients, as it must in its original state, protecting data access and patients' privacy become critical. In addition to the violation of an individual's right to privacy by the improper disclosure of information, the improper *use* of even appropriately held data could result in discrimination by employers and insurers.

Additional privacy concerns surround the Health Insurance Portability and Accountability Act (HIPAA) of 1996, which provides for portability of health insurance, the electronic transfer of data, and development of a unique patient identifier to facilitate data transfers to achieve administrative savings. Linking medical information with life-long personal identifiers raises issues about collection, use and distribution of these data. HIPAA required the executive branch to study means to protect privacy and to make policy recommendations (see "Federal and State Action" below).

Privacy Safeguards

The National Library of Medicine, an executive branch agency with a lead role in facilitating health care applications of the "national information infrastructure," commissioned the Computer Science and Technology Board (CTSB) of the National Research Council to study health data privacy issues. The CTSB's recommendations are detailed in *For the Record: Protecting Electronic Health Information* (National Academy Press, 1997), and include provisions for:

Technical Practices

- Individual authentication of users
- Access controls
- Audit trails
- Physical security and disaster recovery
- Protection of remote access points
- Protection of external electronic communications

Organizational Practices

- Security and confidentiality policies
- Security and confidentiality committees
- Information security officers
- Education and training programs
- Sanctions
- Improved authorization forms
- Patient access to audit logs

Safeguards

Keeping records on paper and in physical files seems comfortable to many people, but it is not without its hazards. Though newer technology can be threatening, it also offers ways, previously unavailable, to protect privacy. For example, data *encryption*, where complex algorithms encode personal identifiers before data are shared, protects the confidentiality of individuals; with traditional paper records, the difficulties of creating non-identifiable data are significant. Electronic *firewalls* within computer systems protect against unauthorized outsiders obtaining information, and *audit trails* allow a systems operator to know who has accessed information and helps determine if there has

been a breach of security. With paper medical records, it is more difficult to be sure that no unauthorized person had accessed the record. Requirements for passwords to access information, along with penalties for sharing pass codes or for improperly disclosing information, can also be effective.

As with the case in Tampa, however, the problem is often human, not technological. Stringent technological protections, accompanied by strong organizational ones, are the best we can do to keep prying eyes away, if medical records are to exist at all.

Summary of Recommendations by HHS Secretary Donna E. Shalala (September 11, 1997)

Boundaries. Use health care information for health purposes only (with a few exceptions) and include all health care providers, payers and service organizations, such as claims processors and pharmacies, under rules governing disclosure.

Security. Prohibit disclosure of patient-identifiable information except when authorized by the patient or as explicitly permitted by legislation, and require those holding information to implement security measures. Prohibit employers acting as payers from using health information for personnel decisions.

Consumer Control. Require providers and payers to inform patients in writing of their information practices, including access, storage, and patients' rights to limit access, authorize disclosure, and see, copy and correct records.

Accountability. Impose criminal penalties for violation of standards, higher when violations are for monetary gain. Permit individuals whose rights have been violated to bring action for damages.

Public Responsibility. Permit limited disclosures of information without patient consent, but with strong protections, for specific national priority activities, including:

- Oversight of the health care system
- Public health
- Health research (including state health data systems)
- Law enforcement

Federal law should provide a minimum standard and should not preempt more stringent state laws.

Federal and State Action

State and federal governments recognize the need for safeguards. In Massachusetts, for example, the Fair Information Practices Act (FIPA) of 1975 protects personal data, and specifically medical data, when the disclosure of such data may constitute an unwarranted invasion of personal privacy. The statute requires security measures — covering accountability, physical security, control of disclosure, and more — to be enacted and enforced by agencies that collect, use, maintain or disseminate personal data for governmental or public functions.

FIPA also provides for penalties for violation of any of its protections, including payment of actual damages, exemplary damages and attorneys' fees. FIPA, the Code of Conduct of the Commonwealth (MGL c. 268A, §23), and many other individual department regulations, policies and procedures protect the privacy of health data. The Executive Office of Health and Human Services is currently reevaluating the scope and effectiveness of these laws and regulations in the agencies under its authority, in the context of its work with the legislative committee considering comprehensive legislation regulating the disclosure of medical records.

Federal policy makers have conducted their own reevaluation. The Health Insurance Portability and Accountability Act of 1996 asked the Secretary of Health and Human Services to recommend federal legislation for the protection of the privacy of individually identifiable health information. To advise the Secretary, the National Committee on Vital and Health Statistics (NCVHS) subcommittee on Privacy and Confidentiality held hearings between January and June 1997, at which 47 experts from public and private organizations testified. The committee considered methods of technological protection, patient access to and amendment of information, authorizations and limitations of disclosure, usefulness of health research, public health, law enforcement, and other issues. HHS Secretary Shalala delivered her recommendations, based largely on the NCVHS report, to Congress on September 11 (see shaded box above).

Decisions

Forty-eight states have laws regarding heath data and privacy protection; new legislation is pending in Massachusetts and other states. Currently, rules such as those in FIPA, the Code of Conduct for Commonwealth employees and individual agency policies provide a basic standard for data security and integrity. While these rules address public agencies, data security standards differ among public and private organizations (physicians, hospitals, health plans, insurers and others). Current levels of security vary, but federal regulations under HIPAA should provide a standard. Such a standard should consider the many uses of data and the appropriate degree of access associated with each use, and protect the data with a combination of encryption and other safeguards, monitoring, and financial and criminal penalties.

That health data can be used for beneficial purposes is beyond dispute. When it is sensitive and accessible, security and privacy concerns are very real. But thoughtful policy measures and security standards that recognize both the risks and benefits of access to data can counter these threats. By understanding the safeguards that are in place, requiring the technical security that computers can provide, being mindful of federal action and making new state policy when necessary, Massachusetts policy makers can create an environment that effects the proper balance between protecting the individual and promoting worthwhile uses of health data.

Further Reading

1. Fact sheet # 8: *How Private is My Medical Information?* Privacy Rights Clearinghouse, San Diego, CA, August 1997.
2. *For the Record: Protecting Electronic Health Information.* Computer Science and Telecommunications Board, National Research Council, Washington, DC: National Academy Press, 1997.
3. *Institute of Medicine, Health Data in the Information Age: Use, Disclosure, and Privacy*. Washington, DC: National Academy Press 1994.
4. *Testimony of Donna E. Shalala, Secretary, United States Department of Health and Human Services,* September 11, 1997 (http://aspe.os.dhhs.gov/admnsimp/).

Did you know?

Preventable Hospitalizations by Diagnosis

	All Ages						*Ages 0-64*					
	Discharges		Total Charges ($millions)		Share of Total Discharges		Discharges		Total Charges ($millions)		Share of Total Discharges	
Diagnostic Group	**FY92**	**FY96**	**FY92**	**FY96**	**FY92**	**FY96**	**FY92**	**FY96**	**FY92**	**FY96**	**FY92**	**FY96**
All PH Conditions	137,328	108,897	838.8	764.5	15%	14%	61,736	43,628	303.0	273.4	10%	9%
Congestive Heart Failure	24,406	23,756	194.7	192.0	3%	3%	3,933	3,595	31.8	31.9	1%	1%
Bacterial Pneumonia	21,115	20,067	162.8	166.7	2%	3%	7,807	6,900	51.2	53.9	1%	1%
Angina	16,787	5,259	65.8	21.7	2%	1%	6,001	1,983	21.1	7.7	1%	0%
Asthma	13,449	9,030	57.9	47.0	1%	1%	10,731	7,368	38.5	35.2	2%	2%
Dehydration	10,351	8,805	56.9	51.1	1%	1%	4,881	3,515	18.1	16.5	1%	1%

* Preventable hospitalizations (PHs) are hospitalizations for ambulatory care sensitive conditions than can be reduced through the timely use of primary health care services. They serve to identify potential barriers to the delivery and/or utilization of more cost-effective primary care services. Total PH figures between tables may not be consistent due to coding errors.

Preventable Hospitalizations by Payer, All Ages—1996

Payer Group	**Discharges**	**Total Charges ($Millions)**	**Share of Total PH Discharges**
All Payers	108,316	764.3	100%
Medicare	64,408	502.5	59%
Medicaid	9,413	64.5	9%
HMOs	11,136	65.2	10%
Blue Cross	8,447	56.1	8%
Commercial Insurers	4,977	29.5	5%
Uninsured	5,242	30.8	5%
Other	4,693	15.7	4%

Source: Massachusetts Division of Health Care Finance and Policy

Staff for this publication:

Ashley Tantum
Kishan Putta
Boyd Gilman
Robert Seifert
Heather Shannon